IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF TEXAS

EL PASO DIVISION

UNITED STATES OF AMERICA,	**§**	
	§	
v.	**§**	**Cause No.: EP-11-CR-2728-KC**
	§	
ANGEL OCASIO,	**§**	
	§	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO COMPEL PRODUCTION OF MATERIALS PERTAINING TO PEER-TO-PEER INVESTIGATIVE SOFTWARE

TO THE HONORABLE JUDGE OF SAID COURT

COMES NOW the United States of America, by and through the United States Attorney for the Western District of Texas and the undersigned Assistant United States Attorney, and submits this Response to Defendant's Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software, and would respectfully show unto this Honorable Court the following:

BACKGROUND INFORMATION

On October 6, 2011, Homeland Security Investigation (HSI) Special Agents executed a duly issued search warrant on defendant's residence at XXXX Fewel Street, El Paso, Texas. At that time, Special Agents seized various items including three computers, two external hard drives, and two USB drives. An on-scene forensic preview of the computer equipment found in Ocasio's room revealed it contained videos depicting the sexual exploitation of minors.

The computers and digital media found at the address on Fewel were taken to the CyberCrimes Computer Forensic Office where Computer Forensic Agent (CFA) Demetrio Medina, along with other CFA's, forensically examined the computer equipment. The examination revealed defendant was in possession of over 100 videos containing child sexual abuse images, many in the range of 25 to 60 minutes in length, including some which had been logged during an initial undercover scan of defendant's IP address by the software referred to as "CPS."

On January 22, 2013, defendant filed a Motion to Suppress [ECF Doc. 85]. On March 11, 2013, the Government responded to the Motion [ECF Doc. 108]. On April 4, 2013, the Court held a hearing on defendant's Motion to Suppress, but defendant presented no witnesses. Instead, defendant was granted leave to file the instant Motion to Compel, which was filed April 8, 2013. [ECF Doc. 117]. The Court ordered the Government to respond no later than April 15, 2013.

ITEMS SOUGHT BY DEFENDANT

Defendant seeks to compel the production of the following items:

1. The source code of the program identified in the affidavit as 'CPS', as well as the source code of any associated programs used to conduct the search in this case. This source code will include any an[d] all commentary included by the programmers.

2. A compiled and fully functional version of any and all software identified in the prior request as implemented by the source code.

3. Technical manuals for any and all software implicated by this investigation, to exclude operating systems and commercially available 'helper' applications for the proprietary software, such as Adobe, Internet Explorer, or the Microsoft Office suite.

4. Training materials presented to the federal government for the previously mentioned software.

5. Details of any software training conducted by the federal government prior to use of any software identified herein, whether designed by the manufacturer or the federal agency.

6. Periodic updates for any software implicated by this request provided to the federal government by the software manufacturer, to include 'bug' fixes, notices directed to software operations or warnings as to known deficiencies in the software.

7. Any information in whatever form, source or nature, which tends to cast doubt on the usefulness, reliability or accuracy of the software identified in identifying suspect child pornography, or which in anyway suggests that the software operates differently than a manual search.

8. A copy of any FAQs (frequently asked questions) directed to the software produced by the manufacturer, if not included in the source code or with the functioning program.

9. And, should the proprietary nature of the software be raised by the Government in objection, a complete copy of the contract entered into between the federal government and the manufacturer.

Of the items requested, only Item 4 (Operating/Training Manual) and Item 9 (Contract) would be in the Government's possession. Of those two items, only the Operating Manual would, conceivably, be relevant and discoverable.

ARGUMENT

In this case, defendant's Motion To Compel relates to two distinct aspects of the proceedings: (1) his suppression motion and (2) his trial. For the reasons set forth below, defendant is wrong to claim his suppression arguments entitle him to the material he seeks. If the evidence law enforcement gathered using CPS bore only on whether agents had probable cause to search defendant's home, disclosure would be unjustified pursuant to either *Brady v. Maryland*, 373 U.S. 83, 87 (1963), or Rule 16.

Moreover, the material which defendant seeks primarily is under the custody and control of a third party – TLO, LLC, a private entity based in Florida. (*See* Exhibit A – Wiltse Affidavit; Exhibit B – Florida Secretary of State documents for TLO, LLC.). The Government has no obligation and no authority to direct a third party to produce materials - either software or other records - over which it does not have possession, custody or control.[1]

Additionally, defendant has failed to make the required prima facie showing of materiality with regards to the information he now requests. Even if defendant could demonstrate the materiality, the materials which are in the Government's possession would be shielded from disclosure under the law enforcement exception to Federal Rule of Criminal Procedure 16.

I. LEGAL STANDARD

The Government has a constitutional obligation to disclose known evidence favorable to the defense when such evidence is material to guilt or punishment. *Brady v. Maryland*, 373 U.S. at 87. A violation occurs if the Government withholds or suppresses such evidence. *Id.*

Nevertheless, the Government is not responsible for information which is not in its possession. *United States v. Hutcher*, 622 F.2d 1083, 1088 (2d Cir.) ("Clearly the government cannot be required to produce that which it does not control and it never possessed"), *cert. denied,* 449 U.S. 875 (1980); *United States v. Josleyn,* 206 F.3d 144, 153-54 (1st Cir. 2000) ("information in the possession of third parties is not imputed to the prosecutor"); *accord United States v. Beaver*, 524 F.2d 963, 966 (5th Cir. 1975) ("But *Brady* clearly does not impose an affirmative duty upon the government to take action to discover information which it does not

[1] Federal Rule of Criminal Procedure 17 sets forth the method by which defendant could attempt to acquire the information he seeks which is in the possession of a third party.

possess.), *cert. denied*, 425 U.S. 905 (1976). Simply put, "*Brady* ... does not require the government to act as a private investigator and valet for the defendant, gathering evidence and delivering it to opposing counsel." *United States v. Tadros*, 310 F.3d 999, 1005 (7th Cir.2002).

Pursuant to Federal Rule of Criminal Procedure 16(a), in addition to its *Brady* requirements, the government must permit the defense:

> To inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Fed. R. Evid. 16(a)(1)(E). A district court's decision whether to order the disclosure of information under Rule 16 is reviewed for abuse of discretion. *United States v. Brown*, 303 F.3d 582, 591 (5th Cir.2002), *cert. denied*, 537 U.S. 1173 (2003) (discussing Rule 16(a)(1)(C), which, after the 2002 amendments, is now Rule 16(a)(1)(E)).

To show the requested items are material to their defense, the defendant must demonstrate the disclosure of the requested evidence would allow them to significantly "alter the quantum of proof" in their favor. *United States v. Reeves*, 892 F.2d 1223, 1226 (5th Cir. 1990). Similarly, information is material to an individual's defense only if it counters the Government's case-in-chief. *United States v. Armstrong*, 517 U.S. 456, 463 (1996). Information not meeting either of those criteria is not "material" within the meaning of the Rule merely because the Government may be able to use it to rebut a defense position. Moreover, information is not material "merely because it would have dissuaded the defendant from proffering easily impeached testimony." *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993).

More importantly, by its plain language, Rule 16(a)(1)(E) does not require the Government to disclose to the defense any and all information material to preparing the defense. Instead, it must only disclose items in its "possession, custody, and control." *See, e.g.*, *Thor v. United States*, 574 F.2d 215, 220-21 (5th Cir. 1978) (defendant not entitled under Rule 16 to address book in the custody of state police); *United States v. Cameron*, 672 F.Supp.2d 133, 137 (D.Me.2009) (Government not required to disclose server files, physical location and addresses of internet service provider's original server, or recorded data not within the Government's possession or control), *aff'd* 669 F.3d 621 (2012) (provider not acting as Government agent in search defendant's account), *cert. denied*, __ U.S. __, 2013 WL 991267 (2013).

In the event it is unclear whether a particular item in the Government's possession is subject to disclosure, the District Court should conduct an *in camera* review of that item. *See, Pennsylvania v. Ritchie*, 480 U.S. 39, 50 (1987) (*in camera* review of disputed evidence protects both parties' rights); *see also United States v. Aref*, 533 F.3d 72, 80-81 (2d Cir. 2008) (district court properly conducted *in camera* review of classified material at issue in discovery dispute), *cert. denied*, 129 S.Ct. 1582 (2009).

II. DEFENDANT'S MOTION TO SUPPRESS DOES NOT PROVIDE GROUNDS FOR HIS MOTION TO COMPEL

Defendant's Motion To Suppress [ECF Doc. 83] is based on two arguments. First, he contends the Government violated the Fourth Amendment by using the CPS software to perhaps access non-public files on his computer. Second, he argues Special Agent Melissa Delarosa's affidavit in support of the search warrant includes false statements and omissions were material to the Magistrate Judge's probable cause determination. Ocasio wrongly suggests these claims justify the discovery he has demanded.

In his Motion To Suppress, Reply To Government's Opposition To Motion To Suppress [ECF Doc. 110], and the instant motion, Defendant reiterates vague assertions regarding an alleged law enforcement computer application, Peer Spectre. Defendant purports to "believe" the Government somehow "accessed" a non-public "system file" on his computer and acquired private information from this "system file" in violation of the Fourth Amendment. *See e.g.* Def. Motion To Suppress at 1, 9.

Although at certain points in his pleadings Ocasio describes this "system file" as "hidden," "hard to find," "not publicly available," and "not designated for sharing," he fails to explain what "system file" and what private information he believes law enforcement obtained from it. Nevertheless, defendant's "hunch" regarding the Government's intrusion into his "system file" is an essential component in his argument in support of his Motion To Compel. *See, e.g.,* Def. Motion to Compel at 2.

In response to Defendant's vague and unsupported assertions, the Government offers the sworn affidavit by the developer of CPS, William S. Wiltse, to assist the Court in making its determinations. (Govt. Ex. A). As defendant's vague and unsupported assertions about CPS and/or Peer Spectre is central to his discovery argument, the Government offers the following information about what CPS is and how it works taken from the Wiltse affidavit (Exhibit A):

> Gnutella is a peer-to-peer network on which a user can send out a search term by typing in a word or a series of words. The user's computer and all of the other recipient computers connected to the Gnutella network communicate in a "request/response manner. In other words, the user's software sends the word search out on the Gnutella network and the software installed and running on the Gnutella-connected recipient computers then searches the

> shared folders on those computers for files whose names contain the searched for word or word. If the software on a connected recipient computer finds a file in that connected computer's shared folder whose file name contains the searched for word or words, the software on that connected recipient computer "responds" to the word search request via the Gnutella network.[2]
>
> CPS, of which Peer Spectre is a component, is software used to access and communicate with the Gnutella network. It was developed by Wiltse to assist law enforcement in child pornography investigations and does so by automating the manual process of typing in and sending out word search requests using terms commonly associated with child pornography files. Otherwise, it submits word search requests in the same way as publicly available software and recipient computers connected to the Gnutella network via their own software respond to those word search requests in the same manner that they would respond to any word search request sent out on the Gnutella network.

Therefore, as Mr. Wiltse states plainly in his affidavit, neither CPS nor its components searches the entirety of a Gnutella-connected computer's contents or perform any other intrusive operation.

Defendant was given the opportunity to litigate his suppression claims at a *Franks* hearing, but elected to present no evidence. It is the Government's position the defendant has failed to overcome even the initial hurdle in connection with his suppression motion and, as such, should not be allowed to rely upon it to get the information sought under this Motion to Compel. Defendant's potentially false and vague assertions cannot support his argument software is "material to preparing the defense" pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E) or exculpatory under *Brady*. In other words, defendant should not be permitted to get through the back door what he cannot get through the front door.

[2] That "response" by the software on the recipient computer includes both the IP address of the recipient computer and the hash value of the file whose file name contained the search term(s).

III. THE GOVERNMENT HAS NO DUTY AND NO AUTHORITY TO DISCLOSE MATERIALS NOT WITHIN ITS POSSESSION, CUSTODY, OR CONTROL.

Most of the information Defendant requests in his pleadings fails to satisfy any of the prerequisites of Rule 16, but more importantly, his requests for information exclusively controlled by TLO are facially invalid due to the fact that it is not "within the government's possession, custody, or control." Fed. R. Crim. P. 16(a)(1)(E). "It is well settled that there is no 'affirmative duty upon the government to take action to discover information which it does not possess."' *United States v. Tierney*, 947 F.2d 854, 864 (8th Cir.1991) (quoting *United States v. Beaver*, 524 F.2d 963, 966 (5th Cir.l975), *cert. denied*, 426 U.S. 905). Moreover, the Government is under no obligation to obtain evidence from third parties. *See United States v. Combs*, 267 F.3d 1167, 1173 (10th Cir.2001) (observing *Brady* does not oblige the Government to obtain evidence from third parties); *see also United States v. Gatto*, 763 F.2d 1040, 1048 (9th Cir. 1985) (Rule 16 does not contain a due-diligence element requiring a prosecutor to search for evidence not within the Government's possession, custody, or control); *United States v. Beaver*, 524 F.2d at 966 ("But *Brady* clearly does not impose an affirmative duty on the Government to discover information which it does not possess.").

In this case, the Government does not have within its possession, custody, or control most, if not all, of the information and documentation sought by defendant. Moreover, under established precedent and the unambiguous language of Rule 16, the Government is under no obligation to seek out this information on defendant's behalf and, as such, it should not be compelled to turn over something it does not have. ''Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel,* 914 F.2d 1215, 1219 (9th Cir. 1990).

IV. THE DOCUMENTS AND OBJECTS CONTROLLED BY TLO ARE NOT MATERIAL TO PREPARING A DEFENSE TO THE GOVERNMENT'S CASE-IN-CHIEF OR RELEVANT TO THE ISSUE OF PROBABLE CAUSE.

A defendant must make a prima facie showing of materiality, that it the information would be helpful to the defense, before he is entitled to obtain requested discovery. *See United States v. Mandel*, 914 F.2d at 1219. To show materiality, the evidence must bear some abstract logical relationship to the issues in the case such that pretrial disclosure would enable the defendant significantly to alter the quantum of proof in his favor. *United States v. Lloyd*, 992 F.2d 348, 350-51 (D.C. Cir. 1993).

Defendant makes no argument the information he seeks from TLO would assist in the preparation of his defense against the government's case-in-chief. *United States v. Armstrong*, 517 U.S. 456, 462 (1996). Rather, Defendant seeks this information as a part of a general fishing expedition to uncover evidence which might assist in his Motion to Suppress.

V. RULE 16 DOES NOT REQUIRE THE GOVERNMENT TO MAKE ALL LAW ENFORCEMENT SOFTWARE AVAILABLE FOR INSPECTION.

In addition to requesting the production of information under the exclusive control of TLO, Defendant appears to be seeking access to Government's software programs and/or software training and documents (*e.g.,* Demand # 3 - technical manuals for *any and all software implicated in this investigation)* (emphasis added). Nothing in the text of Rule 16 or controlling precedent authorizes such a disclosure.

Aside from the discovery of documents and objects as described above, Rule 16 also mandates the disclosure of certain materials related to any scientific examinations or tests the government intends to use in its case-in-chief. Specifically, Rule 16(a)(l)(F) requires the following:

> (F) Reports of Examinations and Tests. Upon a defendant's request, the government must permit a defendant to inspect and to copy or photograph the results or reports of any physical or mental examination and of any scientific test or experiment if:
>
> > (i) the item is within the government's possession, custody, or control;
> >
> > (ii) the attorney for the government knows--or through due diligence could know- -that the item exists; and
> >
> > (iii) the item is material to preparing the defense or the government intends to use the item in its case-in-chief at trial.

Fed. R. Crim. P. 16(a)(1)(F). However, the Rule also makes clear these disclosure requirements do not extend beyond the specific items listed in the Rule and do not "authorize the discovery or inspection of reports, memoranda, or other internal government documents" prepared by the Government in connection with investigating or prosecuting this, or any other, case. Fed. R. Crim. P. 16(a)(2). As such, the Government is obligated to disclose "the results or reports" of any computer forensic examination conducted in the course of this investigation, but Rule 16 does not authorize the disclosure or inspection of proprietary investigative materials, such as Shareaza LE, or the discovery of any underlying data, methods or applications used to generate "the results or reports" described in Fed. R. Crim. P. 16(a)(1)(F).

In *United States v. Price*, 75 F.3d 1440 (10th Cir.), *cert. denied*, 517 U.S. 1239 (1996), the Tenth Circuit roundly rejected the type of ancillary discovery request that Defendant now makes. Evaluating the competing interests and limitations imposed under Rule 16, the Court held the Government did not have to produce: 1) the underlying basis of a chemist's conclusion the substances he tested were methamphetamine; 2) information relating to the reliability of the chemist's equipment; or 3) evidence of chemist's credentials. *Id.* at 1444. In reaching this conclusion, the Tenth Circuit noted that "[t]he language (of Rule 16) is clear on its face. It requires the prosecution to turn over 'results or reports' of scientific tests." *Id*. at 1445 (emphasis added) *citing United States v. Dennison*, 937 F.2d 559, 565-66 (10th Cir. 1991), *cert. denied*, 502 U.S. 1037 (1992) (defining identical terms in Rule 16(b)(1)(B) and (b)(2)).

In *United States v. Ashlock*, 105 Fed. Appx. 581 (5th Cir. 2004), *vacated on other grounds* 543 U.S. 1136 (2005), the Fifth Circuit Court of Appeals relied on *Price* in upholding the trial court's decision not to strike expert testimony when the Government failed to provide detailed protocols of tests employed by forensic experts. *Id.* at 586 ("Rule 16(a) does not instruct the government to provide detailed step-by-step information regarding the routine protocols employed by the expert in performing the tests discussed in the report."). This interpretation has also been widely adopted by federal courts around the nation. *See e.g., United States v. Iglesias*, 881 F.2d 1519, 1523-24 (9th Cir. 1989), *cert. denied*, 493 U.S. 1088, (1990) (discovery obligation satisfied by turning over lab reports regarding analysis of substance and would not be required to turn over log notes, protocols, and other internal documents of chemists who worked on the analysis); *United States v. Uzenski*, 434 F.3d 690, 709 (4th Cir. 2006) (no requirement to disclose laboratory notes because final report already disclosed).

VI. THE *BUDZIAK* DECISION IS NOT CONTROLLING IN THIS CASE

The defendant has raised *United States v. Budziak,* 697 F.3d 1105 (9th Cir. 2012), as determinative of his request. However, that case is distinguished easily from the instant matter.

In *Budziak*, the Ninth Circuit Court of Appeals concluded the trial court erred in declining to permit review of the software (eP2P) which had been utilized by the Federal Bureau of Investigation (FBI) and sought by the defendant as it might have been beneficial to the defense. The Court remanded the case for the trial court's review and determination whether the materials sought might have affected the jury's deliberations. What is not clear from the appellate decision is upon what grounds the trial court could have ordered it's disclosure. That question easily is answered by a review of the trial court record.

In the trial court, *United States v. Budziak,* CR 08-00284-RMW, N.D. Ca (San Jose Division), the defendant brought a Motion to Compel under Rule 16(a)(1)(E) seeking:

1. The technical specifications and documentation regarding the enhanced version of the LimeWire peer to peer (P2P) software designed by the FBI and used in the investigation of this case.

2. An order requiring the prosecution to provide an installable copy of the eP2P software used in this case for review by computer forensic expert Ronald Short and Mr. Budziak's counsel. This order is to be subject to whatever protective orders the Court finds appropriate.

3. In the alternative, an order compelling the government to provide to the defense a complete written description of the capabilities of the government's enhanced LimeWire software program used in this case in June 2007, in comparison to the LimeWire software available to the public in June 2007.

Motion to Compel, filed in *United States v. Budziak* as ECF Doc. 115 (attached hereto as Exhibit C for the Court's convenience); *see also*, *Id.* at ECF Doc. 134.[3]

While at first blush this may appear to provide support to defendant's claim, a closer reading reveals one decisive point which actually defeats Ocasio's claim – that is, the eP2P

[3] Defendant Budziak also brought a Motion to Suppress on the same grounds as alleged herein. The Motion was denied by the trial court, as well [ECF Doc. 165] and that ruling was not disturbed on appeal.

software was proprietary to the FBI. That point was born out further by the declaration of FBI Supervisor Special Agent Jacqueline Dougher filed by the Government in *Budziak:*

> 2. I am the program manager for the use of the eP2P program. In this role, I am responsible for teaching law enforcement officers how to utilize this investigative tool, the investigative use of the eP2P program, the continued development of the software, and the dissemination of the program throughout the FBI and other law enforcement agencies.
>
> 3. The software program that has come to be known as eP2P, is specialized software *developed by the FBI* for the investigation of illegal distributions through the use of peer-to-peer software that provides for file sharing among participants. …
>
> 4. *The FBI* protects the eP2P software with a non-disclosure agreement prohibits [sic] law enforcement agencies from disseminating the software. …
>
> …
>
> 5. *The FBI* protected the source code of the eP2P software from disclosure to even FBI agents and law enforcement officers utilizing the software in investigations by locking the source code. …

Declaration of Jacqueline Dougher filed in *Budziak* as ECF Doc. 63-4 (attached hereto as Exhibit D for the Court's convenience) (emphasis added).

It is clear from a reading of the *Budziak* documents the computer program sought by the defendant therein was developed by and in the exclusive control of the government. Such is not the case herein. As noted in the Declaration of William Wiltse the material which defendant seeks was not developed by the Government and is not, and never has been, in the custody or control of the Government:

> 2. I am the developer of the law enforcement computer application known as "Peer Spectre". This application was created in conjunction with Flint Waters of the Wyoming Division of Criminal Investigations as part of an investigative effort formerly known as Peer Precision. This effort, now known as the Child Protection System (CPS), focuses on the development of software tools to identify computers trading files depicting the sexual abuse of children and training law enforcement officers in their use. *The Child Protection System was developed by*

> *TLO, LLC, a private company located in Boca Raton, Florida.* I am currently employed as the Director of Law Enforcement Programming at TLO and oversee all development activities related to the aforementioned Child Protection System. I am also certified as an instructor for the Child Protection System and regularly provide instruction to law enforcement officers prior to providing them access to the system.
>
> …
>
> 10. The source code used by the Child Protection System and related applications has not been, and will not be, distributed to any law enforcement officer or agency, to include Special Agent Melissa De La Rosa or Special Agent Nicolas Marquez of the Department of Homeland Security, Immigration and Customs Enforcement.

Exhibit A.

This is not a distinction without a difference. As the Government had custody and control of the eP2P program, it was discoverable under Rule 16 and *Brady*. Herein, however, the program is copyrighted to a private company and is not in the Government's "possession, custody, or control." Fed.R.Crim.P 16(a)(1)(E). Based on the foregoing, the Government respectfully submits *Budziak* has no legal precedent in this matter.

VII. THE INFORMATION WITHIN THE GOVERNMENT'S POSSESSION IS SHIELDED FROM DISCLOSURE BY THE LAW ENFORCEMENT PRIVILEGE.

Several circuits have "recognized a qualified privilege against compelled government disclosure of sensitive investigative techniques." *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir.), *cert. denied*, 484 U.S. 913 (1987); *In re U.S. Department of Homeland Security*, 459 F.3d 565 (5th Cir. 2006). These courts have noted disclosure of the "precise specifications" of certain surveillance methods "will educate criminals regarding how to protect themselves against police surveillance," *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986), and "perhaps unduly jeopardize the security of ongoing investigations," *Cintolo,* 818 F.2d at

1002. Because “[t]he potential price to be paid by law enforcement is heavy, [it] should not be assessed without good reason.” *Id.; see also United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982) (refusing to permit disclosure of the location of a police surveillance post). That standard is met here.

Even assuming Defendant somehow could demonstrate materiality as required by *Armstrong* or knowing falsehood as required by *Franks*, his discovery request still is barred by the well-established law enforcement privilege for those items within the Government’s possession and control. This privilege is designed "to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *In re Dep't of Investigation of City of New York*, 856 F.2d 481, 484 (2d Cir. 1988). Its bar is "based primarily on the harm to law enforcement efforts which might arise from public disclosure of ... investigatory files." *See Black v. Sheraton Corp. of America*, 564 F.2d 531, 541 (D.C. Cir. 1977); *see also United States v. Winner*, 641 F.2d 825, 831 (10th Cir. 1981); *United States v. Van Horn*, 789 F.2d 1482, 1496 (11th Cir.) (electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised), *cert. denied*, 479 U.S. 854 (1986). Moreover, it has been specifically adapted to prevent the discovery of information which, if disclosed, "will enable criminals to frustrate future government surveillance." *United States v. Cintolo*, 818 F.2d at 1002.

As Mr. Wiltse explains in his affidavit, the Child Protection System is a group of software tools developed by TLO, a private company located in Boca Raton, Florida. Exhibit A, ¶ 2. TLO only provides their software to “specifically trained and licensed law enforcement” officers and its use is restricted to such officers in the performance of their law enforcement duties. *Id.* ¶ 3. Whenever a trained and licensed law enforcement officer uses the system, the program submits lead information to TLO’s server. *Id.* ¶¶ 4-5, 11. According to Mr. Wiltse, there is no way to prevent this from occurring. *Id.* If an untrained and unlicensed person were to use CPS or any of its suite of programs to communicate with a peer-to-peer network, that person’s use could generate leads to law enforcement officers who would believe, wrongly, the leads were generated by the work of trained law enforcement personnel.

In addition, the software submits its leads to the TLO server via a specific web address, or Uniform Resource Locator (URL). According to Mr. Wiltse, an unlicensed, non-law enforcement user could uncover the URL of TLO’s server with certain software which is freely available. Once exposed, TLO’s server would be susceptible to digital intrusion. *Id*. ¶ 12.

Finally, an unlicensed, non-law enforcement user could also expose the manner in which CPS communicates with the law enforcement server at TLO. A person could use this information to intentionally submit false information to TLO’s law enforcement server, creating false leads. *Id*. ¶ 13.

For these reasons, allowing untrained, unlicensed persons from the defense team to use CPS or any of its components would put ongoing investigations at significant risk and imperil future investigations. The Court, therefore, should find such disclosure is not permitted pursuant to the law enforcement privilege.

VIII. DEFENDANT'S SPECIFIC REQUESTS

Based on the foregoing principles, the Government responds to defendant's specific requests as follows:

1. **The source code of the program identified in the affidavit as 'CPS', as well as the source code of any associated programs used to conduct the search in this case. This source code will include any an [sic] all commentary included by the programmers.**

2. **A compiled and fully functional version of any and all software identified in the prior request as implemented by the source code.**

3. **Technical manuals for any and all software implicated by this investigation, to exclude operating systems and commercially available 'helper' applications for the proprietary software, such as Adobe, Internet Explorer, or the Microsoft Office suite.**

The evidence sought by defendant under these requests is not within the Government's possession, control or custody and, therefore, is not subject to Rule 16. Likewise, there is no *Brady* violation as the evidence is not being suppressed by the government; it cannot suppress what it does not have and which is known by the defendant to be in the possession of a third party.

4. **Training materials presented to the federal government for the previously mentioned software.**

The government is in possession of one training manual which may be responsive to this request. Nevertheless, under Rule 16, it is incumbent upon a defendant to make a prima facie showing of "materiality." *United States v. Buckley*, 586 F.2d 498, 506 (5th Cir. 1978), *cert. denied*, 440 U.S. 982 (1979); *see also United States v. Budziak*, 697 F.3d at 1111. "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense." *Id.* Indeed, courts have generally held Rule 16 allows for discovery of law enforcement manuals only where those manuals are material. *See United States v. Dongjun Li*, 2011 WL 8035118, at *2-3 (D.N. Mar. I. Oct. 24, 2011) (unredacted sections of DEA field manual not material); *United States v. Hasan,* 747 F. Supp. 2d 642, 682 (E.D. Va. 2010) (NCIS manuals not material), *cert. denied*, 133 S.Ct. 982 (2013); *United States v. Norita*, 708 F. Supp. 2d 1043, 1054-55 (D.N. Mar. I. 2010)(DEA field agent manual not material); *United States v. French*, 2010 WL 1141350, at *6-7 (D. Nev. Mar. 22, 2010)(operating manual of third party software not material). Nevertheless, even if the manual was relevant and material, the Government submits the law-enforcement privilege applies to most, if not all of the manual.

When dealing with the discovery of documents possibly covered by this privilege, the Fifth Circuit has instructed the district court to review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies to the documents at issue. "In making its determinations, the Court must balance the government's interest in confidentiality against the litigant's need for the documents." *In re U.S. Department of Homeland Security, supra,* 459 at 570–71. The Government is prepared to submit the manual to the Court for *ex parte, in camera* review, if so required, along with proposed redactions and bases therefor.

5. Details of any software training conducted by the federal government prior to use of any software identified herein, whether designed by the manufacturer or the federal agency.

Defendant again fails to articulate the materiality of the requested information, even assuming it was in the Government's possession.

6. Periodic updates for any software implicated by this request provided to the federal government by the software manufacturer, to include 'bug' fixes, notices directed to software operations or warnings as to known deficiencies in the software.

7. Any information in whatever form, source or nature, which tends to cast doubt on the usefulness, reliability or accuracy of the software identified in identifying suspect child pornography, or which in anyway suggests that the software operates differently than a manual search.

Again, the Government has no such information in its possession, especially as to updates and "bug" fixes, etc., which again would be in the possession of the third party, TLO. Additionally, the Government has no information which "tends to cast doubt on the usefulness, reliability or accuracy of the software" or "in anyway suggests that the software operates differently than a manual search." Moreover, the Affidavit of William Wiltse also indicates TLO has no such information. (Exhibit A, ¶ 14).

8. A copy of any FAQs (frequently asked questions) directed to the software produced by the manufacturer, if not included in the source code or with the functioning program.

Again, this information is not in the Government's possession, but rather in the possession of a third party.

9. And, should the proprietary nature of the software be raised by the Government in objection, a complete copy of the contract entered into between the federal government and the manufacturer.

Defendant once again fails to articulate how the requested information material, that is how the production of a contract between the Government and a third party contractor would enable him significantly to alter the quantum of proof in his favor. See *United States v. Head*, 586 F.2d 508, 512 (5th Cir. 1978), *citing Calley v. Callaway*, 519 F.2d 184 (5th Cir. 1975) ("We required that Calley establish some indication that disclosure would have enabled him to significantly alter the quantum of proof in his favor.") Defendant herein makes no allegation the production or inspection of these materials would yield evidence he did not in fact commit the crimes as alleged in the Indictment. At best, defendant attempts to justify this request for discovery by making an indirect *Franks* challenge to the search warrant affidavit, which an improper use of Rule 16.

CONCLUSION

WHEREFORE, the United States respectfully requests this Court find the Government does not have possession, custody or control of the information held by TLO, a private corporation and thus not discoverable under Fed. R. Crim. P. 16 and to find the law enforcement privilege precludes disclosure of any information in the Government's possession under the circumstances.

WHEREFORE, premises considered, defendant's motion is not well-taken and should be denied without hearing.

Respectfully submitted,

ROBERT PITMAN
UNITED STATES ATTORNEY

By: /s/
J. BRANDY GARDES
Assistant United States Attorney
CA Bar No. 144770
700 E. San Antonio, Ste. 200
El Paso, Texas 79901
(915) 534-6884

CERTIFICATE OF SERVICE

I hereby certify that on the 15th day of April, 2013, a true and correct copy of the foregoing instrument was electronically filed with the Clerk of the Court using the CM/ECF System which will transmit notification of such filing to the following CM/ECF participant:

Michael Gorman, AFPD
Shane McMahon, AFPD
Federal Public Defenders Office
700 E. San Antonio, 4th Floor
El Paso, Texas 79901

Attorneys for Defendant

/s/
J. BRANDY GARDES

IN THE UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF TEXAS

EL PASO DIVISION

UNITED STATES OF AMERICA, §
§
v. § **Cause No.: EP-11-CR-2728-KC**
§
ANGEL OCASIO, §
§

ORDER

On this day came to be considered the Defendant’s Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software [ECF Doc. 117], and the Government’s Response thereto [ECF Doc. 118]. After due consideration, the Court is of the opinion the motion should be DENIED.

Accordingly, it is hereby ORDERED Defendant’s Motion to Compel Production of Materials Pertaining to Peer-to-Peer Investigative Software [ECF Doc. 117], is hereby **DENIED**.

SIGNED and ENTERED this ___ day of ____________________, 2013.

____
KATHLEEN CARDONE
UNITED STATES DISTRICT JUDGE